UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/876,568
Filing Date: June 07, 2001
Appellant(s): CA ET AL.

Kevin M. Mason
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/16/06 appealing from the Office action mailed 08/09/05.

(1) Real Party in Interest

A statement identifying by name the real party in interest as AGERE SYSTEMS GUARDIAN CORP is contained in the brief.

(2) Related Appeals and Interferences

The brief indicated no related appeals and interferences, which directly affect or be directly affected by or have a bearing on the decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

- Cromer et al. (U.S. Patent No. 6021493), *hereinafter Cromer*,
- Sanders et al. (U.S. Patent No. 5231375), *hereinafter Sanders,*
- Lam (U.S. Patent No. 6140923),
- Minasi (Mark Minasi, "Mastering Windows NT Server 4, 6th edition, 1999, ISBN: 0782124453), pg. 378, 380 and 434,
- Thurrott (Paul Thurrott, "What's new in Windows 2000 RC2 Reviewed", http://www.winsupersite.com/reviews/win2k_rc2_whatsnew.asp), pg. 1-3,
- Computer Dictionary ("Charles J. Sippl and Roger J. Sippl "Computer Dictionary and handbook", 3rd edition, 1980, ISBN: 0-672-21632-9).

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

Claims 1,10, 17, 22, 26-29 and 31-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Thurrott (Paul Thurrott, "What's new in Windows 2000 RC2 Reviewed", http://www.winsupersite.com/reviews/win2k_rc2_whatsnew.asp).

Thurrott teaches monitoring a network connection and generating an alarm if the network connection is disconnected (Network disconnect cue section).

Windows 2000 RC2 taught by Thurrott is implemented on computers comprising memory and processors and codes.

Claim Rejections - 35 USC § 102 or 103

Claims 1, 7-10, 12, 17, 22, 26-29 and 31-32 are rejected under 35 U.S.C. 102 as being anticipated by or, in the alternative, under 103(a) as obvious over Cromer et al. (U.S. Patent No. 6021493).

As per claims 1, 7-9, 26-28 Cromer et al. teach a system and method for detecting when a computer system is removed from a network (col. 2 lines 17-19). In particular Cromer et al. teach LAN software application running on the remote computer system or server that has a list of LAN clients addresses. The software polls client computers and if it does not get a response back after a predetermined number of retries, it generates an alarm resulting in alerting a LAN administrator that a client is now not attached to the LAN (col. 7 lines 31-49). This reads on: "detecting removal of a device connected to a network by a network connection comprising monitoring the network connection and generating an alarm if the network connection is disconnected.

Cromer et al. does not explicitly teach that an alarm is generated in the removed device. However, disconnecting the remote computer system (or server) would result in lack of response to sent polls by the software application hosted on the computer system. As a result the alarm would have been generated on the device disconnected from the network. Even if disconnection of the remote

computer system did not result in generation of the alarm it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement such a modification. One of ordinary skill in the art would have been motivated to perform such a modification in order to warn about a computer (in this case the remote computer system) being removed from a network.

Claims 17, 22 and 31-32 are substantially equivalent to claim 1; therefore claims 17, 22 and 31-32 are similarly rejected.

As per claim 12 Cromer et al. teach waiting for a response for a predefined time interval (col. 8 lines 35-40).

As per claims 10 and 29 Cromer et al. teach LAN communication utilizing IP addresses (col. 8 line 47).

Claim Rejections - 35 USC § 103

Claims 2-3, 13-14, 18-19 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Sanders et al. (U.S. Patent No. 5231375) and in further view of Lam (U.S. Patent No. 6140923).

Cromer et al. teach generating an alarm if a network connection is disconnected.

As per claims 2, 13, 18, 23 Cromer et al. do not teach that the generated alarm generates an audio output and do not teach preventing a volume of an audio output of the device from being reduced below a predefined minimum level.

Sanders et al. teach a device (Sanders et al., theft detection and alarm system, Sanders et al., Fig. 1 object 1010) connected to a network (Interface Unit 1020, Data transmission System 1030, Interface Unit 1040, Theft and alarm system

monitor 1050 and database1060, Fig. 1) by a network connection, that produces an audible alarm signal in the device (that prevents a volume of an audio output of the device from being reduced below a predefined minimum level) when a network connection is disconnected (Sanders et al., Fig. 2, col. 5 lines 33-38), and Lam provides a motivation to combine (Lam, col. 48-51).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to generate an alarm in the removed device as taught by Sanders et al. One of ordinary skill in the art would have been motivated to perform such a modification in order to draw attention to the device.

Preventing a volume of an audio output of the device from being reduced below a predefined minimum level (as implemented in Sanders et al.'s invention) is implicit, since lowering the volume could prevent drawing attention to the device.

As per claims 3, 14, 19 and 24 the device implementing audible alarm system taught by Sanders et al. prevents the device from being turned off (Sanders et al., Fig. 6 and col. 11 lines 46-49). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend *Cromer's* invention by preventing the device from being turned off given the benefit of efficient network administration e.g. monitoring the network devices while preventing terminating the monitoring invented by *Cromer* that would occur if the device was turned off.

Claims 3, 14, 19 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Minasi (Mark Minasi, "Mastering Windows NT Server 4, 6th edition, 1999, ISBN: 0782124453)

Cromer teaches a system and method for detecting when a computer system is removed from a network. Cromer does not teach preventing the turning off a device.

Minasi teaches assigning rights to users that grant or deny access to certain objects (resources) such as turning off a device (Minasi, pg. 378 §3 and, shut down rights pg. 380, turning off a device in particular). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement Minasi's teaching preventing the turning off a device in order to prevent said devices from being turned off mistakenly and thereby causing false alarms.

Claims 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Pearce (U.S. Patent No.6308272).

Cromer et al. teach monitoring a network connection as discussed above.

Cromer et al. do not explicitly address how said monitoring step is activated.

As per claim 4 Pearce teaches monitoring that is set to activate automatically in a passive manner (provide security during a selected period of time, col. 6 lines 61-68). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure monitoring being activated automatically in a passive manner as taught by Pearce in order to activate monitoring at times where the threat of a network problem is most likely to occur (e.g. after work hours) and in order to avoid false alarms (avoid hours of scheduled network maintenance, re-configuration etc.). Also, it is implicit that the period time is

selected by the user who must manually configure and activate the system in order for monitoring to be automatically activated in a passive manner, thus reading on claim 5.

Claims 6, 11, 15-16, 20-21, 25 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer et al. (U.S. Patent No. 6021493) in view of Sobell (Mark G. Sobell, "A practical guide to the UNIX system, 3rd Edition, 1997, ISBN: 0805375651).

Cromer et al. teach monitoring a network connection as discussed above.

Cromer et al. do not teach a generating step being prevented by entering a password.

Sobell teaches using a password to perform administrative tasks (login as the Superuser, pg. 493).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use password as taught by Sobell in order to perform administrative tasks limited only to authorized (administrative and supportive) staff. One of ordinary skill in the art would have been motivated to perform such a modification in order to be able to perform administrative tasks such as device relocations, troubleshooting, network upgrade etc. without triggering false alarms.

(10) Response to Argument

On page 4 appellant contests independent claims 1, 17, 22 and 31 as rejected under Thurrott.

Appellant argues that Thurrot's visual cue alerts are unlikely to be effective as an alarm to alert one or more individuals to a theft, as would be apparent to a person of ordinary skill in the art. Appellant concludes by stating that "a person of ordinary skill in the art would not interpret the visual cue disclosed by Thurrott as an alarm for indicating a theft".

The examiner points out that *Thurrott* clearly discloses the alarm as cited in the claim language.

Computer Dictionary provides the definition of an "alarm" to be "a signal, by display or audio device, which signifies that an error has occurred, or an emergency condition exists that is interfering or could interfere with the proper execution or completion of a program" *(Computer Dictionary, pg. 12).*

Thurrott's icon alarming a user that a network cable became unplugged *(Network disconnect cue section and Fig. 3)* unambiguously reads on generating an alarm since unplugging the cable results in a condition that can and does interfere with the proper execution or completion of at least programs requiring a network connection *(e.g. back up of critical files to a remote computer)* and alarming the user about the condition. Disconnecting a cable providing a network connection to a device removes the device from the network, regardless of how critical it is to maintain a connection between the device and other network devices still connected to the network.

In regard to appellant's argument that *Thurrott's* reference does not explicitly address "indication of a theft" the examiner points out that "indication of theft" is not present in any of the claims 1, 17, 22 and 31. Claims 1, 17, 22 and 31 recite only in the preambles "removal of a device connected to a network".

Summarizing, *Thurrott* clearly teaches monitoring network connection of a device and generating an alarm in the (removed) device if the network connection is disconnected.

On page 4-5 appellant contests independent claims 1, 17, 22 and 31 rejected under Cromer.

Appellant argues that Cromer does not disclose or suggest generating an alarm in the removed device. Appellant then presumes that Cromer teaches away from the present invention by teaching to install an alarm outside of the protected device.

Before addressing appellants' arguments the examiner points out that in *Cromer's* invention **the remote computer system or server 34** as well as **the software application** (Cromer, col. 7 line 35) **read on "a device"** recited in the claim limitations. Computers *(clients, servers, remote computers, network nodes etc.)* perform particular functions thanks to software that is implemented on the computers. As a result, in regard to the current application, a method implemented by software cited by *Cromer* should not be considered as a method implemented by some separate network entity

but rather as a method implemented by a device (the remote computer system or server) on which the software is executed.

For example, as cited by appellant regarding *Cromer's* col. 7, lines 41-49 the functions performed by software application are actually actions performed by a remote computer or server 34 *(hereinafter a device)* that runs the software *(col. 7 lines 34-35)*.

Thus, reading *Cromer's* citation the remote computer system or server 34 as well as software application should be considered as matching the term "the device" used in the claim language and the term should be considered distinct from "a client" recited by *Cromer.*

The term "client" recited by *Cromer* corresponds to a second device *(claim 12)* and/or a remote device *(claim 17)*.

The claim language calls for monitoring a network connection of a device and generating an alarm in the *(removed)* device if the network connection is disconnected.

Network consists of all of the computer's residing on the same network. Thus, both: clients and the device *(a remote computer or a server 34)* cited by Cromer reside on the same network should be considered as "devices connected to the network".

As a result generating an alarm in a device *(taught by Cromer)* that is a result of removing the device from the network reads on "generating an alarm in the removed device".

As per *Cromer's* teaching:

> *"when the client receives this packet it transmits a packet back to the LAN indicating it is still on the LAN. If the software application gets a response back then it just moves to the next client. If the software application does not get a response back after a predetermined number of retries, it indicates to the LAN administrator though a message that the client at this location is now not attached to the LAN and can be assumed missing or stolen" (Col. 7, lines 41-49)*

Appellant argues (pg. 5) that *Cromer* discloses that the software application that receives the response from the client (and not the client) is the application that sends a message to the LAN administrator. Appellant concludes the arguments with an assertion that *Cromer* does not teach "generating an alarm in the removed device" if the network connection is disconnected.

The examiner points out that although the software application indeed receives responses from the client, appellant's assertion that *Cromer* does not teach "generating an alarm in the removed device" is incorrect.

As previously discussed the application software is not an independent entity but it is an entity utilized by a device *(the remote computer system or server, Cromer col. 7 lines 34-35)*. With this in mind, the examiner would like to point out the facts regarding events that take place in *Cromer's* invention.

As clearly disclosed by *Cromer* and cited by appellant *("...if the software application does not get a response back after a predetermined number of retries...")* the device *(utilizing the software application)* sends network enquiries *(polls a network client)* and based on the outcome *(response or no response)* it determines a status of the network connection *(connection between the device and the network)*. As a result, the response coming from the network client signifies the fact that there is a network connection.
In other words, the device in *Cromer's* invention verifies a status of network connection and if no network connection *(no response)* is detected an alarm is generated.

The examiner also emphasizes that not only clients but also the device is connected to the network. As a result disconnecting a network connection removes the device from the network, and consequently prevents the device from receiving the responses.

The reason is very simple: the requests directed to network clients will never reach the network and thus it will not reach the clients either. Even if the requests were sent prior to disconnecting the network connection, as soon as the device is removed from the network any returning responses from clients will fail to reach the device.
The lack of responses results in the device generating an alarm.

Cromer clearly teaches generating an alarm on the device *(Cromer, col. 9 lines 21-23)*.
The alert generated and sent out by the device reads on the alarm since it is a signal

indicative of an emergency condition. Note that the "client is missing" recited in *Cromer* in col. 9 lines 21-23 is based on no response from the client *(col. 7 lines 44-48).* Also, one should not focus on the fact that due to the problem with the network connection the generated alarm may not reach the intended destination but rather the focus should be on the fact that the alarm signal is generated if the device (or a client) is removed from the network.

As per "monitoring a network connection", as previously shown, removing the network connection results in generating an alarm. Of course, discovering that the network connection is removed can only be possible in the case where the network connection is monitored. In *Cromer's* invention such a monitoring is achieved by polling *(that is sending a response and receiving a response, Cromer, col. 7 lines 32-49)* network clients.

Summarizing, *Cromer* clearly teaches a method for detecting removal of a device connected to a network by a network connection *(a remote computer or a server 34 using software application polls a network, Cromer, col. 7 lines 31-49 and col. 9 lines 19-23)*, comprising monitoring network connection of a device *(is the device connected or not connected to the network; that is does the device receive responses from the network, e.g. from a network client, Cromer, col. 7 lines 40-46)* and generating an alarm *(generate an alarm notifying about the disconnected network*

connection) in the removed device if the network connection is disconnected *(Cromer, col. 9 lines 21-23).*

On page 5 appellant contests the rejection of independent claims 1, 17, 22 and 31. *In particular appellant argues that Cromer and Thurrott alone or in combination do not disclose or suggest generating an alarm in the removed device if the response is no longer received or not received within a predefined time interval.*

As per the received response that is no longer received, Cromer clearly indicates that when the removed device *(implementing the software)* does not receive a response from the network the device is aware that there is no present network connection and this is what triggers the alarm on the removed device *(col. 7 lines 44-48).* Of course, removing the network device from the network *(disconnecting the network connection)* will result in no longer receiving any responses from the network.

As per a predefined time interval, *Cromer* discloses a predetermined time that each request for the response is sent *(col. 7 lines 37-40)* and that the device waits for the response and only after it "does not get a response back after a predetermined number of retries" it assumes the network connection has been disconnected *(Cromer, col. 7 lines 44-48).*

On page 6 appellant continues to contest the rejection of independent claims 1, 17, 22 and 31.

On page 6-8 appellant discusses Sanders et al., Lam, Minasi, Pearce and Sobell with respect to claims 1, 17, 22 and 31.

Since neither of the cited references was used against the independent claims 1, 17, 22 and 31 the examiner does not traverse applicant's arguments.

On page 8-9 appellant contests the rejection of dependent claims 2, 13, 18 and 23 rejected under Cromer in view of Sanders and Lam.

Appellant argues that Thurrott, Cromer, Sanders, Lam, Minasi, Pearce and Sobell, alone or in any combination do not disclose or suggest preventing a volume of an audio output of the device from being reduced below a predefined minimum level.

Appellant also specifically cites Sander's col. 5 lines 33-38 as evidence of not teaching preventing a volume of an audio output of the device from being reduced below a predefined minimum volume.

Cromer's invention has been discussed above.

Since *Cromer* did not disclose an alarm in audible form *(an audio output of the device)* the examiner introduced *Sanders* that extends *Cromer's* invention with an audio output of the device that is utilized for an audible alarm signal in the device *(Sanders, col. 5*

lines 33-38). Furthermore, the examiner disclosed *Lam's* invention that provides motivation to combine *Cromer's and Sander's* inventions.

In particular, *Lam* stresses an importance of an audible alarm signal *(Lam, col. 2 lines 27-29 and col. 1 lines 52-58).*

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend *Cromer's* invention with an audio output sounding an audible alarm signal given the benefit of strong notification of occurrence of the alarm condition.

Cromer in view of *Sander* and *Lam* do not explicitly recite preventing a volume of an audio output of the device from being reduced below a predefined minimum level. However, preventing a volume of an audio output of the device from being reduced below a predefined minimum level would have been obvious to one of ordinary skill in the art at the time of applicant's invention given the fact that lowering the volume of the alarm could defeat the purpose of the audible alarm, especially since an unauthorized person *(e.g. a thief)* would have a particular interest in disabling the audible alarm.

In addition, the examiner once again points to *Sander's* alarm system that produces an audible alarm. As clearly disclosed in col. 11 lines 49-55 *Sander* is particularly concerned with affecting an alarm *(including volume)* and takes special precaution to prevent silencing *(that would also read on lowering the volume)* the alarm system.

Summarizing, *Cromer* in view of *Sander* and *Lam* teach an audio output of the device strongly notifying about an emergency condition. Furthermore preventing reduction of a volume below a predefined minimum level would have been obvious to one of ordinary skill in the art at the time of applicant's invention given the fact that reducing the volume could defeat the purpose of the audio alarm implementation.

On page 9-10 appellant contests rejection of dependent claims 3, 14, 19 and 24. *Appellant argues that the Cromer, Sanders, Lam and Minasi do not disclose or suggest preventing the device from being turned off.*

Cromer's invention has been discussed above.
Since *Cromer* did not explicitly teach preventing the device from being turned off, the examiner introduced *Minasi* who stresses the importance of effective administration of networks with a plurality of computers *(Minasi, "System Policies: Central Registry Control", pg. 434)*. The discussion of the administration is continued on pg. 378 where *Minasi* discusses user rights *(Minasi, "User Rights and Object Permissions")*. On pg. 380 *Minasi* concludes by providing variables that could be administrated. One of these variables is "Shut down the system" that can be granted to users.

The examiner points out that the existence of "shutting down the system" variable means that just as "shutting down the system" can be granted, the "shutting down the

system" privilege can be revoked. As a result, *Minasi* inherently teaches "preventing shutting down the system".

Cromer's invention aims towards theft protection as well as network monitoring *(Cromer, col. 7 lines 31-49)*. Turning the device off (shut down the device) would defeat the purpose of *Cromer's* invention.

As a result, extending *Cromer's* invention with preventing the device from being turned off would have been obvious to one of ordinary skill in the art at the time of applicant's invention. One of ordinary skill in the art would have been motivated to perform such a modification given the benefit of efficient network administration e.g. monitoring the network devices while preventing terminating the monitoring invented by *Cromer* that would occur if the device was turned off.

In addition, the examiner once again points to *Sander's* alarm system that produces an audible alarm. As clearly disclosed in col. 11 lines 49-55 *Sander* is particularly concerned with the possibility of turning off the alarm system. Not only does the alarm system device *(Fig. 2-3, object 1010)* have no output allowing the device to be turned off, but *Sander* also explicitly discloses an internal battery power that prevents turning off the device by removal of a power cord *(col. 11 lines 49-55)*.

Thus, extending *Cromer's* invention with preventing the device from being turned off would have been obvious to one of ordinary skill in the art at the time of applicant's invention. One of ordinary skill in the art would have been motivated to perform such a

modification given the benefit of efficient network administration e.g. monitoring the network devices while preventing terminating the monitoring invented by *Cromer* that would occur if the device was turned off.

Summarizing, *Cromer* in view of *Minasi* teach preventing the device from being turned off given the benefit of efficient network administration that includes monitoring the network devices while preventing termination of the monitoring invented by *Cromer* that would occur if the device was turned off.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Peter Poltorak

Conferees:

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Kim Vu,

Justin Darrow.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Computer Dictionary & HANDBOOK

Charles J. Sippl
and
Roger J. Sippl

THIRD EDITION
SECOND PRINTING—1980

International Standard Book Number: 0-672-21632-9
Library of Congress Catalog Card Number: 79-67133

Printed in the United States of America.

Preface

Because personal computers are now cost-effectiv
hours of training, more and more systems are being
nesses. As a result, they are reaching users who are
use of computers. These users, especially those in
need to learn exactly what the move to microelectr
search for answers, they are perplexed by the jarg
industry, and they discover that they must quick
computer language. They must study and master
it is becoming very unbusinesslike, and even unf
what is a 64K RAM, a semiconductor, or a bubble

When the first computer is installed in a busines
and managers of the business apprehensive, but
office and administrative personnel are suspicious a
changes that take place. Management must help
and knowledgeable approach to explaining what
they must know something about the "mysterious"

Filling the need for this information is the purp
tion to the definitions of terms, of equal value a
serve as a "state-of-the-art" guide section that pro
essential elements of computer concepts that we a
to time.

This is a "browsing" dictionary. It is a tutorial
be brief. Many definitions and explanations are lo
so. Users of this book can easily and leisurely bro
supplemental entries of an "area," such as "data
detail about the products, procedures, problems,
tions. While we have included many definitions r
the art of programming, the basics of electronics,
components of systems, we have limited them to a
them as clear and "unconfusing" as the literature
product manuals, applications notes, inventor e
descriptions, seminar notes, and conference proceed

conversion (ADC) function. The devices permit the construction of high performance ADCs at a fraction of the cost of comparable modular units. With this subsystem, the critical analog processing is done on the monolithic chip, and the less critical digital system of counters and gates is left for the system designer to implement.

ADIS — Abbreviation for A Data Interchange System.

adjacency — 1. Relates to character recognition and printing conditions. Reference lines designate spacing between two consecutive characters. 2. A condition in character recognition in which two consecutive characters, either printed or handwritten, are closer than the specified distance.

adjacent channel — A channel whose frequency band is adjacent to that of the reference channel.

adjacent-channel interference — Such interference or "noise" occurs when two modulated carrier channels are situated or placed too close together in frequency so that one or both sidebands extend from one channel into the other.

adjacent-channel selectivity — Receivers have characteristics which govern their ability to reject signals or channels adjacent to that of the desired signals.

adjustment, character — The address adjustment in which the literal used to modify the address has reference to a specific given number or group of characters.

administrative data processing — An expression usually meaning business data processing such as the recording, classifying, or summarizing of transactions, activities, events, etc. Usually of a financial nature, or the collection, retrieval, or control of such items.

admissible mark — *See* mark, admissible.

ADP (Automatic Data Processing) — 1. Pertaining to equipment such as EAM (Electronic Accounting Machines) and EDP (Electronic Data Processing) equipment units or systems. 2. Data processing performed by a system of electronic or electrical machines so interconnected and interacting as to reduce to a minimum the need for human assistance or intervention.

ADPE — Abbreviation for Automatic Data Processing Equipment.

ADPS — Abbreviation for Automatic Data Processing System.

AFIPS — Abbreviation for American Federation of Information Processing Societies, an association of American data processing groups formerly called AFID.

agenda — The set of control-language statements used to prescribe a solution path or run procedures; an ordered list of the major operations constituting a procedure for a solution or computer run. (This usage corresponds roughly to the ordinary "agenda" for a meeting.)

A ignore B gate, negative — *See* gate, B ignore A negative.

A implies B gate — *Same as* gate, B OR NOT A.

A implies B gate, negative — *Same as* gate, A AND-NOT B.

alarm — A signal, by display or audio device, which signifies that an error has occurred, or an emergency condition exists that is interfering or could interfere with the proper execution or completion of a program.

alarm, audible — This is an audio signal which indicates that a predetermined condition has been met or detected, that a malfunction has occurred in the equipment, or that a program error or a problem condition exists.

alarm display — A visual display signal such as on a crt or radar screen which would alert the operator to conditions which require attention.

alarm-repeated transmission — An audible alarm which sounds after three successive failures to transmit (or receive) a line.

alertor — A device to watch the man who watches the machine. The alertor consists of a small box connected to a large floor pad laced with wires. Any movement on the pad keeps the box content. But, should there be no movement from the operator during a suspicious interval of time, the alertor concludes he is either inattentive or napping, and sounds an alarm.

algebra, Boolean — *See* Boolean algebra.

algebraic expression — A statement expressed in various symbols, signs, and abbreviations following mathematic

rules and syntax to designate variables, constants, functions, and rules.

algebraic language — *See* language, algebraic.

Algebraic Language, International — *See* Language, International Algebraic.

ALGOL — 1. ALGOrithmic Language. An arithmetic language by which numerical procedures may be precisely presented to a computer in a standard form. The language is intended not only as a means of directly presenting any numerical procedure to any suitable computer for which a compiler exists, but also as a means of communicating numerical procedures among individuals. The language itself is a result of international cooperation to obtain a standardized algorithmic language. The International Algebraic Language is the forerunner of ALGOL. 2. ALGebraic Oriented Language (some authors). The international procedural language.

ALGOL 10 — A FORTRAN-like programming language that offers the scientific advantages of FORTRAN and advanced algorithmic processing capabilities. Used mainly on time-sharing systems. (Digital Equipment Corp.)

ALGOL 68 — Much like ALGOL 10, this version of the language offers input-/output facilities more prone for the batch environment. Used mainly on batch systems, although it is also used on some select time-sharing systems. (IBM.)

algorithm — A defined process or set of rules that leads and assures development of a desired output from a given input. A sequence of formulas and/or algebraic/logical steps to calculate or determine a given task; processing rules.

algorithm convergence — An algorithm is said to converge if it is certain to yield its solution in a finite number of steps. It is a much stronger requirement than the mathematical convergence of the sequence of obtained function values.

algorithmic — Pertaining to a constructive calculating process usually assumed to lead to the solution of a problem in a finite number of steps.

algorithmic language — *Same as* ALGOL.

algorithmic routine — That specific routine which directs the computer in a program to solve a problem in a finite or specified number of steps, but not rely-

ing on a tr
solution a
and must
swer.

algorithm, f
ming algo
applied to
tered prob
cifies the
processed
tive of th
method, ri
sign a solu
or class of

algorithm, sel
is included
the execut
algorithm
user's qua
which this

algorithm tr
rules, spe
used to o
language t
done by t
tional met

alias — 1. A
something
is being u
ondary n
slang such
etc., whic
or primar
point whe
lowed to

A-light — A
monitors
ity check

aligned wor
systems,
dressed as
structions
most byte
has an ev
are aligne
resulting
high and
the alignm
improve
doubling
instructio

alignment —
compone
terrelatio
pecially t
ponents i

allocate — T
the main

What's new in Windows 2000 RC2 Reviewed

Windows 2000 Release Candidate 2 (RC2, build 2128) is the final major release before the product is released to manufacturing, a feature-complete look at the most ambitious operating system project ever undertaken by Microsoft. As such, this release is marked most obviously by the extremely subtle changes between it and RC1: There just aren't a lot of obvious differences (Figure 2), though that's a good thing when you're trying to ship a product. But even with the similarities, I was able to uncover the following differences in RC2:

Changes to multiprocessing

Between the release of RC1 and RC2, Microsoft announced that all of the Server family products would be updated to support better symmetrical multiprocessing (SMP). So Server Edition now supports four processors (up from two) and Advanced Server supports eight (up from four). This was done largely to calm fears about the dropping of the Alpha platform, which had previously been Microsoft's high-end solution.

Network disconnect cue

Networking simplification has always been a goal in Windows 2000 and with RC2 a new visual cue has been added to alert the user when the machine is disconnected from the network. Even when you choose to not display a tray icon when connected, an icon will appear to alert you should the network cable or Ethernet card become unplugged (Figure 3). When the network connection is physically reconnected, the icon disappears.

My Network Places updates

Long-time Windows 2000 users are used to the "nag screens" you see when you navigate to the *Program Files*, *Winnt*, and *System32* folders. In RC2, a new nag screen has been added to the *Entire Network* folder (Figure 4, found within *My Network Places*). This was done to reduce network traffic since the view from this folder could cause hundreds or even thousands of machines to be polled on a large network.

If you're running Windows 2000 on a domain, the "Computers Near Me" icon has been removed, though it remains on workgroup systems. Microsoft's rationale for this change is that there are far too many machines in a typical domain and displaying them all when the user clicked this icon was time and resource intensive. After all, this was the reason these computer icons were removed from the root of My Network Places to begin with.

Add/Remove Programs tweaks

When you choose *Add/Remove Windows Components* in *Add/Remove*

Screenshots

Figure 1: Windows 2000 Pro RC2 startup screen.

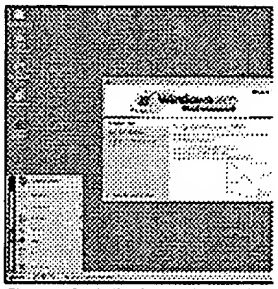

Figure 2: Windows 2000 Pro RC2 desktop.

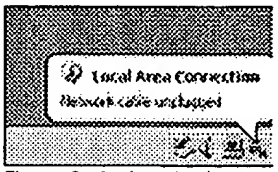

Figure 3: An icon in the tray when the network is physica unavailable.

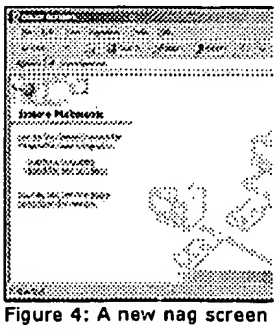

Figure 4: A new nag screen Network.

Programs, a "Please wait" alert lets you know that the system is at least doing something while you wait for the dialog to appear (Figure 5). In earlier builds, there was just an awkward pause, making one wonder whether they had actually clicked the option properly.

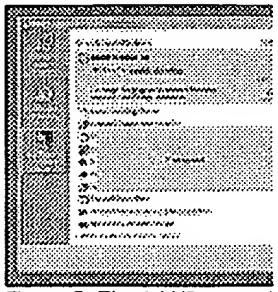

Figure 5: The Add/Remove components choice is prefac "Please wait" alert.

Internet Explorer 5.01
Windows 2000 RC2 contains the latest version of Internet Explorer, version 5.01 (build 5.00.2919.3800), which includes numerous bug fixes as well as a few new features (Figure 6). IE 5.01 will continue to be updated over the next few months and then will be finalized just before Windows 2000 goes gold.

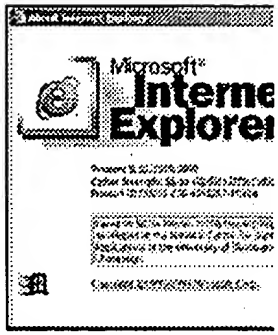

Figure 6: Internet Explorer !

APM power management removed from Server family
For reasons that completely escape me, and despite repeated attempts by me and others to have this feature reinstated, Microsoft stripped APM power management from Server and Advanced Server (it still exists in Professional, and the Server products still support the new and more powerful ACPI power management). This means that any servers built before January 1, 1999 will have no power management at all, leaving many developers in the lurch.

I understand that most servers don't actually need power management, but the vast majority of Windows 2000 systems out there today were built before 1/1/99. I think this was a mistake, though not a critical one.

MDAC 2.5
Windows 2000 RC2 includes the final release of Microsoft's Data Access Components (MDAC) version 2.5, which includes new features and numerous bug fixes. One of the coolest new features is the ability to open an ADO recordset from a standard Web URL, a feature that will be extended by the next version of SQL Server, code-named "Shiloh." Also, Windows 2000 includes the basic SQL Server client software, allowing Windows 2000-based ADO, OLE-DB, and ODBC clients to easily access SQL Server data on other servers.

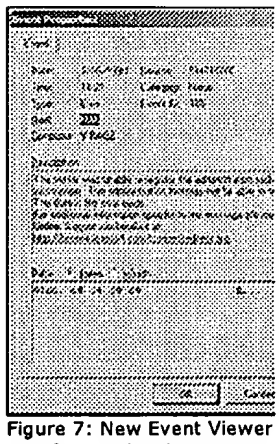

Figure 7: New Event Viewer interface makes it easy to w individual events.

Event Viewer UI update
The use interface of the Event Viewer has been updated to make it easier to navigate between events and their properties (Figure 7). And a new hyperlink feature, linking an error event to the appropriate description on Microsoft's Web site is a nice touch.

Conclusions
As you can see by this short list, there isn't much new to Windows 2000 RC2, but then that's a good thing: Sure, bugs have been fixed and new drivers have been implemented, but to the end user, Windows 2000 has remained a virtual constant since the Beta 3 release back in April. That makes sense, since the product has been feature frozen for some time. So, as an end user, RC2 is a little boring because it looks and feels the same as the other releases we've been using for some time now. But it doesn't take much perspective to realize that this build is something special, an early look at the final OS to come.

And that day isn't far off: Windows 2000 is ready to go final.

THE #1 BEST-SELLING NT BOOK OF ALL TIME OVER 350,000 COPIES IN PRI

MASTERING™ WINDOWS® NT® SERVER 4

SIXTH EDITION

MARK MINASI

ON THE CD:
THE COMPLETE BOOK IN SEARCHABLE PDF FORMAT, PLUS NT TOOLS AND UTILITIES

THE COMPLETE GUIDE TO ENTERPRISE NETWORKING WITH NT—ENHANCED AND EXPANDED TO COVER SERVICE PACK 4

#1 NT AUTHORITY MARK MINASI'S TIME-TESTED METHODS FOR BUILDING TROUBLE-FREE NT NETWORKS

COVERS NT SERVER 3.51 AND NT SERVER 4 THROUGH SERVICE PACK 4

NETWORK PRESS® SYBEX

MARK MINASI'S TECHNICAL SOLUTIONS®

Associate Publisher: Gary Masters
Acquisitions Manager: Kristine O'Callaghan
Acquisitions & Developmental Editor: Neil Edde
Editors: Peter Weverka, Lee Ann Pickrell, Brenda Frink, Nancy Conner
Project Editor: Dann McDorman
Technical Editor: Donald Fuller
Book Designer: Catalin Dulfu
Graphic Illustrators: Patrick Dintino, Catalin Dulfu, Tony Jonick
Electronic Publishing Specialists: Cyndy Johnsen, Kate Kaminiski
Production Coordinators: Charles Mathews, Shannon Murphy
Indexer: Matthew Spence
Companion CD: Ginger Warner
Cover Designer: Archer Design
Cover Photographer: FPG International

Screen reproductions produced with Collage Complete.
Collage Complete is a trademark of Inner Media Inc.

SYBEX, Network Press, and the Network Press logo are registered trademarks of SYBEX Inc.
Mastering is a trademark of SYBEX Inc.

TRADEMARKS: SYBEX has attempted throughout this book to distinguish proprietary trademarks from descriptive terms by following the capitalization style used by the manufacturer.

The CD interface music is from GIRA Sound AURIA Music Library © GIRA Sound 1996.

Library of Congress Card Number: 98-88945
ISBN: 0-7821-2445-3

Manufactured in the United States of America
10 9 8 7 6 5 4

TIP

By default, you can never lock out the built-in Administrator account, no matter how many failed logon attempts are made. However, the *NT Resource Kit* contains a program named PASSPROP which can render the default Administrator account vulnerable to lockout. Just run PASSPROP from the command line at any domain controller like so: **passprop /adminlockout**, and then reboot.

The "Forcibly disconnect remote users from server when logon hours expire" option is tied in to the available logon hours you specified when you created the user account. If this option is selected, the user is disconnected from all connections to any of the domain's servers once the logon hours expire.

Not selecting this option enables the user to stay connected once the logon hours expire, but no new connections will be permitted. Checking "User must log on in order to change password" makes it impossible for the user to change her password after it's expired.

User Rights and Object Permissions

User access to network resources—files, directories, devices—in NT Server is controlled in two ways: by assigning *rights* to a user that grant or deny access to certain objects (for example, the ability to log on to a server), and by assigning *permissions* to objects that specify who is allowed to use objects and under what conditions (for example, granting read access for a directory to a particular user).

Consider the groups Users and Administrators. What makes administrators different from users? Well, administrators can log on right at the server; users can't. Administrators can create users and back up files; users can't. Administrators are different from users in that they have rights that users don't have. The central thing to remember here is that the very thing that separates one group in NT from another mostly has to do with the rights the groups have. You control who gets which rights via the User Manager for Domains.

Rights generally authorize a user to perform certain system tasks. For example, the average user can't just sit down at an NT server and log on right at the server. The question, "Can I log on locally at a server?" is an example of a right. "Can I back up data and restore data?" "Can I modify printer options on a shared printer?" These are also user rights. User rights can be assigned separately to a single user, but for reasons of security organization, it is better to put the user into a group and define which rights are granted to the group. You manage user rights in User Manager for Domains.

TIP

FIGURE 6.19:

User Rights Policy dialog

Check the arrow box next to the currently displayed user right to see the entire list of regular user rights. By clicking one of the rights, you can see the groups and users who currently have been granted that particular right. In the figure, you can see that the right "Access this computer from network" has been granted to the Administrators and Everyone group.

The regular rights used in NT Server are

Access this computer from network Allows a user to connect over the network to a computer.

Add workstations to domain Makes machines domain members.

Back up files and directories Allows a user to back up files and directories. As mentioned earlier, this right supersedes file and directory permissions.

Change the system time Grants a user the right to set the time for the internal clock of a computer.

Force shutdown from a remote system Note that, although presented as an option, this right is not currently implemented by NT Server.

Load and unload device drivers Lets a user add or remove drivers from the system.

Log on locally Allows a user to log on locally at the server computer itself.

Manage auditing and security log Gives a user the right to specify what types of events and resource access are to be audited. Also allows viewing and clearing the security log.

Restore files and directories Allows a user to restore files and directories. This right supersedes file and directory permissions.

Shut down the system Grants a user the right to shut down Windows NT.

Take ownership of files or other object Lets a user take ownership of files, directories, and other objects that are owned by other users.

NOTE Ownership is explained in Chapter 7.

System Policies: Central Registry Control

Over the years, Microsoft has accomplished many things in some areas but hasn't been too successful in others. NT has superbly implemented multitasking, a large memory model (when was the last time you worried about whether or not something would fit into 640K?), and a vastly improved user interface. Put simply, users have just *got* to love many of the things that NT offers.

Support people, on the other hand, haven't got so much to like. In the typical modern corporation, each corporate support person must ride herd on hundreds or sometimes thousands of PC desktops, solving problems, installing upgrades, and giving advice. But modern PC operating systems don't offer much help to those support folks. Want to remotely control a PC over a network? Remotely install a new piece of software? Can't do any of that with the tools that come in the box with NT. What happens when you've got NT half-installed and the Setup program goes into the weeds? You have a completely useless computer—half installed is no better than newborn as far as NT (or just about any other PC operating system, for that matter) goes.

All that's supposed to change with Windows 2000 Server and its associated Zero Administration Windows. But you don't have to wait until Windows 2000 Server for support relief—there are two tools built into NT 4 that make it a bit easier to support and control hundreds of workstations from a single point. The first is *user profiles*, which you read about earlier in this chapter. The other tool is *system policies*.

So what's a system policy and why do you care? That's the topic of the next few dozen pages, but first let's look at the overview. System policies are essentially *central control of users' Registries*.

Why Would You Want to Control Registries?

As you know, virtually *everything* that has anything to do with controlling an NT machine (and a Windows 95 machine, for that matter) is in the Registry. But I'll bet you didn't know all of the things that you can control with the Registry; certainly some of these surprised *me*. Here are a few examples:

- The contents of the folders that a user sees when she clicks the Start button
- Which icons and controls appear on the Desktop

Restricting What Programs a User Can Run with Explorer Policies

RestrictRun is another mildly complex Registry setting; it's incredibly powerful. You can use it to say to the Windows interface, "Do not run any programs unless they are on the following list." For example, you could say, "The only programs that this user can run are Word and Internet Explorer." RestrictRun is another 1 or 0 Registry setting: 0 says, "Don't restrict which programs this user can run," and 1 says, "Only allow this user to run the programs listed in HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Windows\Policies\Explorer\RestrictRun." *That* key is just a list of applications that can run, and it consists of as many value entries as you like, all of type REG_SZ, and one application to a value. The name of the first entry must be, simply, 1, and again should contain the file name of the acceptable program. The second would be named 2, and so on. It's probably easiest to see an example, as in Figure 6.67. In that example, I've allowed this user to run (respectively) the Calculator, Internet Explorer, Word, and Command Prompt.

FIGURE 6.67:
Using RestrictRun to limit user application